Customer Story

NETRISE

Enhancing Firmware Security and QA Efficiency for a Global Broadband Solutions Provider

A global broadband solutions provider delivering video, Wi-Fi, and connected-home platforms to service providers worldwide sought to strengthen the security and quality assurance (QA) of the firmware powering its devices. As its portfolio expanded and customers demanded higher speed, reliability, and security, the company recognized the need to validate firmware integrity with the same rigor applied to product performance.

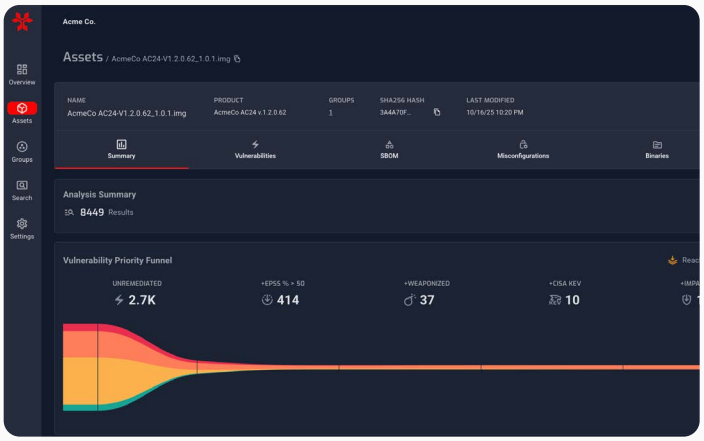
The provider began evaluating scalable solutions for firmware security after observing the positive results another operator achieved using the NetRise Platform.

Challenge

In order to ensure the security of the devices they sell, the provider needed to:

- Validate firmware from original equipment manufacturers (OEMs) before release to customers
- Identify vulnerabilities and other risk, such as hard-coded secrets and misconfigurations, without access to the device's source code
- Equip QA engineers with clear, actionable visibility into software components
- Strengthen collaboration with OEM and chipset partners to reduce risk from upstream suppliers

To meet these challenges, the company sought a partner that could move quickly - providing not just a platform, but a knowledgeable team ready to demonstrate, teach, and guide adoption from day one.



The NetRise Platform

Solution

The provider evaluated several tools and selected NetRise® for its strong binary analysis capabilities after an exceptional onboarding experience. A dedicated demo environment, tailored instruction on interpreting results, and responsive engagement throughout purchasing and implementation made the decision straightforward.

The provider integrated the NetRise Platform® into its QA workflow. Each firmware release candidate now undergoes binary analysis as a standard step in the validation process. The team has analyzed more than a dozen firmware images to date, leveraging NetRise's execution-aware reachability to identify vulnerabilities in components that auto-run at system startup. This visibility helps the QA team concentrate remediation on the issues that present real exposure.

NetRise enables the provider to prioritize findings—identifying vulnerabilities that are accessible through the network, present on the CISA Known Exploited Vulnerabilities list, or that carry a high Exploit Prediction Scoring System (EPSS) rating. With this context, QA engineers can address the issues most likely to affect customers and product quality.

These prioritized insights have enabled more productive coordination with OEMs and chipset partners. The team can now demonstrate which vulnerabilities could pose real exposure versus those that are non-exploitable in deployed systems, creating more focused, data-driven conversations about remediation and component updates.

Results

By integrating NetRise into its QA process, firmware security is validated and prioritized, achieving measurable improvements in speed, confidence, and visibility:

Repeatable QA Analysis

Firmware scans are now a standard, automated step in every release, giving QA teams a reliable view into software composition and security posture before deployment.

Smarter Vulnerability Prioritization

With insights powered by execution-aware reachability, teams can focus on vulnerabilities in components that execute under real runtime conditions, streamlining QA efforts and reducing unnecessary rework.

Improved OEM Collaboration

Shared visibility has enabled more constructive, data-driven discussions with OEM and chipset partners, replacing speculation with clear priorities for remediation and validation.

Consumer Confidence

Using kernel configuration intelligence, teams can separate kernel CVE noise from real exposure, helping service-provider customers understand which issues truly require action first.

Together, the provider and NetRise have built a more efficient, evidence-based QA process that balances product performance, customer satisfaction, and security assurance.

Why It Matters

For service providers, every connected device represents both an opportunity and a responsibility. As homes become more intelligent and networks more distributed, operators must ensure that every component, from routers to set-top boxes, delivers security as reliably as it delivers connectivity.

With NetRise integrated into its QA process, the provider can assure customers and partners that the code within its products meets both performance and security expectations. The partnership reflects the company's ongoing commitment to quality, innovation, and customer trust, reinforced by objective data and continuous validation.

The provider maintains that trust at scale via its partnership with NetRise, giving its engineering and QA teams deeper visibility into firmware composition, vulnerability reachability, and component integrity.

"The NetRise team jumped in immediately and worked alongside us to understand our environment and goals. Their support and platform visibility have made a real difference in how we validate firmware and communicate with our partners."

— **Engineering Leader**, Global Broadband Solutions Provider

See how binary analysis strengthens QA and supply chain assurance.

Explore the NetRise Platform

